

PRIMO ESERCIZIO DI W3D4 (PING DA KALI PER WINDOWS 7 DOPO L' IMPOSTAZIONE DEL FIREWALL)

```
kali-linux-2024.1-virtualbox-amd64 [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
File Actions Edit View Help
(kali@kali)-[~]
$ ping <IP_Windows_7>

zsh: parse error near `\\n'

(kali@kali)-[~]
$ ping 192.168.50.102
PING 192.168.50.102 (192.168.50.102) 56(84) bytes of data.
64 bytes from 192.168.50.102: icmp_seq=1 ttl=128 time=1.83 ms
64 bytes from 192.168.50.102: icmp_seq=2 ttl=128 time=1.71 ms
64 bytes from 192.168.50.102: icmp_seq=3 ttl=128 time=3.59 ms
64 bytes from 192.168.50.102: icmp_seq=4 ttl=128 time=7.53 ms
^C
— 192.168.50.102 ping statistics —
4 packets transmitted, 4 received, 0% packet loss, time 3399ms
rtt min/avg/max/mdev = 1.706/3.661/7.525/2.352 ms

(kali@kali)-[~]
$
```

WIRESHARK PROVA PACCHETTI CATTURATI SU ETH0

Kali-linux-2024.1-virtualbox-amd64 [In esecuzione] - Oracle VM VirtualBox

File Macchina Visualizza Inserimento Dispositivi Aiuto

*eth0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	fe80::dd1c:4f67:7c3...	ff02::c	SSDP	208	M-SEARCH * HTTP/1.1
2	3.004281324	fe80::dd1c:4f67:7c3...	ff02::c	SSDP	208	M-SEARCH * HTTP/1.1
3	7.005556920	fe80::dd1c:4f67:7c3...	ff02::c	SSDP	208	M-SEARCH * HTTP/1.1
4	9.495837896	fe80::dd1c:4f67:7c3...	ff02::1:2	DHCPv6	150	Solicit XID: 0x009e97 CID: 000100012dceddf70800275422c7
5	10.006780167	fe80::dd1c:4f67:7c3...	ff02::c	SSDP	208	M-SEARCH * HTTP/1.1
6	10.489819082	fe80::dd1c:4f67:7c3...	ff02::1:2	DHCPv6	150	Solicit XID: 0x009e97 CID: 000100012dceddf70800275422c7
7	12.492932226	fe80::dd1c:4f67:7c3...	ff02::1:2	DHCPv6	150	Solicit XID: 0x009e97 CID: 000100012dceddf70800275422c7
8	13.009273715	fe80::dd1c:4f67:7c3...	ff02::c	SSDP	208	M-SEARCH * HTTP/1.1
9	16.492334651	fe80::dd1c:4f67:7c3...	ff02::1:2	DHCPv6	150	Solicit XID: 0x009e97 CID: 000100012dceddf70800275422c7
10	17.009614970	fe80::dd1c:4f67:7c3...	ff02::c	SSDP	208	M-SEARCH * HTTP/1.1
11	20.010326267	fe80::dd1c:4f67:7c3...	ff02::c	SSDP	208	M-SEARCH * HTTP/1.1

Frame 2: 208 bytes on wire (1664 bits), 208 bytes captured (1664 bits) on interface eth0, id 0000 33 33 00 00 00 0c 08 00 27 54 22 c7

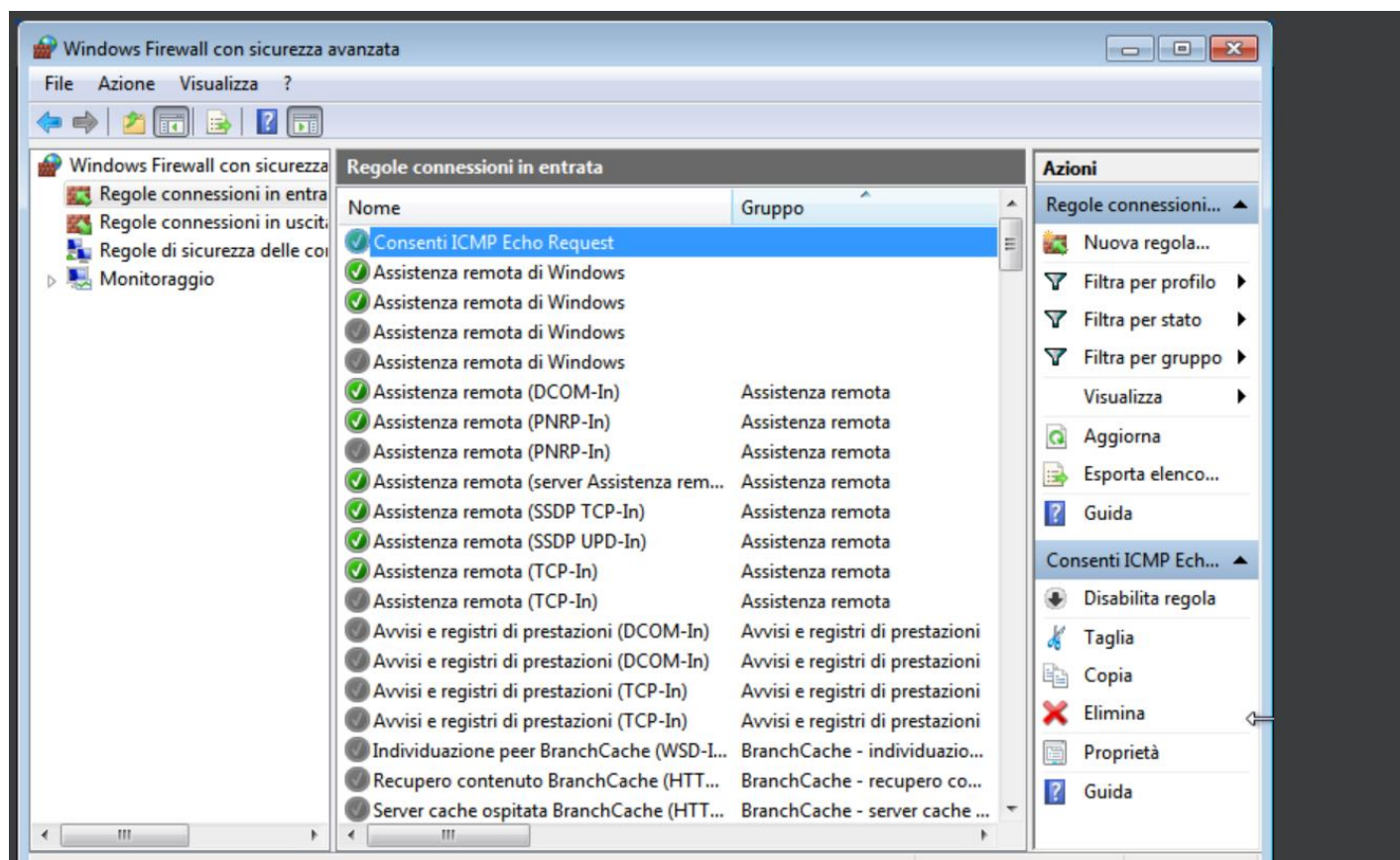
Ethernet II, Src: PCSSystemtec_54:22:c7 (08:00:27:54:22:c7), Dst: IPv6mcast_0c (33:33:00:00:00:0c)

Internet Protocol Version 6, Src: fe80::dd1c:4f67:7c35:11f6, Dst: ff02::c

User Datagram Protocol, Src Port: 58277, Dst Port: 1900

Simple Service Discovery Protocol

SCREEN DI UNA PARTE DELL' IMPOSTAZIONE POLICY FIREWALL

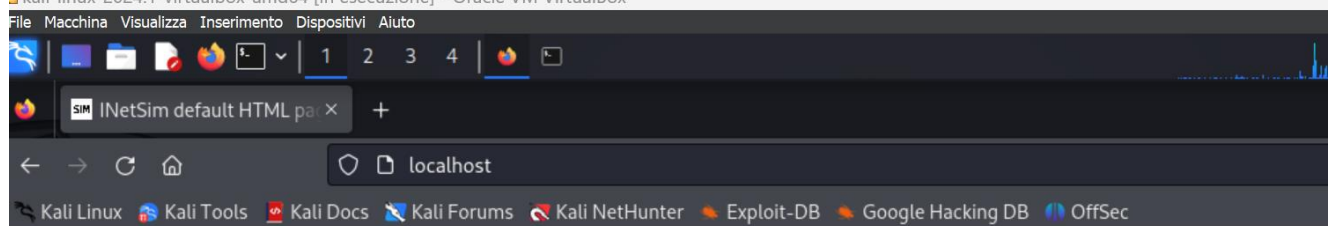


SUDO INETSIM

kali-linux-2024.1-virtualbox-amd64 [In esecuzione] - Oracle VM VirtualBox

```
File Macchina Visualizza Inserimento Dispositivi Aiuto
kali@kali: ~
File Actions Edit View Help
└─$ sudo inetsim
[sudo] password for kali:
INetSim 1.3.2 (2020-05-19) by Matthias Eckert & Thomas Hungenberg
Main logfile '/var/log/inetsim/main.log' does not exist. Trying to create it ...
Main logfile '/var/log/inetsim/main.log' successfully created.
Sub logfile '/var/log/inetsim/service.log' does not exist. Trying to create it ...
Sub logfile '/var/log/inetsim/service.log' successfully created.
Debug logfile '/var/log/inetsim/debug.log' does not exist. Trying to create it ...
Debug logfile '/var/log/inetsim/debug.log' successfully created.
Using log directory: /var/log/inetsim/
Using data directory: /var/lib/inetsim/
Using report directory: /var/log/inetsim/report/
Using configuration file: /etc/inetsim/inetsim.conf
Parsing configuration file.
jConfiguration file parsed successfully.
=== INetSim main process started (PID 2438) ===
Session ID: 2438
Listening on: 127.0.0.1
Real Date/Time: 2024-05-24 13:36:37
Fake Date/Time: 2024-05-24 13:36:37 (Delta: 0 seconds)
Forking services ...
* dns_53_tcp_udp - started (PID 2448)
deprecatd method; prefer start_server() at /usr/share/perl5/INetSim/DNS.pm line 69.
Attempt to start Net::DNS::Nameserver in a subprocess at /usr/share/perl5/INetSim/DNS.pm line 69.
* time_37_tcp - started (PID 2463)
* daytime_13_tcp - started (PID 2465)
* smtps_465_tcp - started (PID 2452)
* daytime_13_udp - started (PID 2466)
* smtp_25_tcp - started (PID 2451)
* finger_79_tcp - started (PID 2460)
* ntp_123_udp - started (PID 2459)
* irc_6667_tcp - started (PID 2458)
```

kali-linux-2024.1-virtualbox-amd64 [In esecuzione] - Oracle VM VirtualBox



This is the default HTML page for INetSim HTTP server fake mode.

This file is an HTML document.

WIRESHARK PROVA PACCHETTI CATTURATI SU ANY

The screenshot displays a Kali Linux virtual machine environment. The primary application is Wireshark, which is capturing network traffic on the 'eth0' interface. The packet list pane shows 18 packets, with the first packet (No. 1) selected. This packet is an ARP request from 192.168.50.102 to 192.168.50.101. The packet details pane shows the Ethernet II header and the ARP request structure. The packet bytes pane shows the raw data in hexadecimal and ASCII. A terminal window in the background shows the command 'arp -a' output.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	PCSSystemtec_54:22:...		ARP	62	Who has 192.168.50.101? Tell 192.168.50.102
2	0.000017461	PCSSystemtec_1e:36:...		ARP	44	192.168.50.101 is at 08:00:27:1e:36:4a
3	0.000436026	192.168.50.102	192.168.50.101	NBSS	62	NBSS Continuation Message
4	0.000478808	192.168.50.101	192.168.50.102	TCP	80	34558 → 445 [ACK] Seq=1 Ack=2 Win=249 Len=0 TSval=2827125
5	5.208049890	PCSSystemtec_1e:36:...		ARP	44	Who has 192.168.50.102? Tell 192.168.50.101
6	5.208810354	PCSSystemtec_54:22:...		ARP	62	192.168.50.102 is at 08:00:27:54:22:c7
7	120.075542975	PCSSystemtec_54:22:...		ARP	62	Who has 192.168.50.101? Tell 192.168.50.102
8	120.075559793	PCSSystemtec_1e:36:...		ARP	44	192.168.50.101 is at 08:00:27:1e:36:4a
9	120.075882137	192.168.50.102	192.168.50.101	TCP	62	[TCP Keep-Alive] 445 → 34558 [ACK] Seq=1 Ack=1 Win=257 Le
10	120.075899279	192.168.50.101	192.168.50.102	TCP	80	[TCP Keep-Alive ACK] 34558 → 445 [ACK] Seq=1 Ack=2 Win=24
11	125.334933674	PCSSystemtec_1e:36:...		ARP	44	Who has 192.168.50.102? Tell 192.168.50.101
12	125.335464625	PCSSystemtec_54:22:...		ARP	62	192.168.50.102 is at 08:00:27:54:22:c7
13	218.066100370	192.168.50.102	192.168.50.255	BROWSER	245	Local Master Announcement WINDOWS7, Workstation, Server,
14	240.151156696	PCSSystemtec_54:22:...		ARP	62	Who has 192.168.50.101? Tell 192.168.50.102
15	240.151169101	PCSSystemtec_1e:36:...		ARP	44	192.168.50.101 is at 08:00:27:1e:36:4a
16	240.151485942	192.168.50.102	192.168.50.101	TCP	62	[TCP Keep-Alive] 445 → 34558 [ACK] Seq=1 Ack=1 Win=257 Le
17	240.151499403	192.168.50.101	192.168.50.102	TCP	80	[TCP Keep-Alive ACK] 34558 → 445 [ACK] Seq=1 Ack=2 Win=24
18	245.394659328	PCSSystemtec_1e:36:...		ARP	44	Who has 192.168.50.102? Tell 192.168.50.101

Frame 1: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) on eth0
 Linux cooked capture v1
 Address Resolution Protocol (request)